DOI: 10.53477/2668-6511-22-10

FUNCTIONS AND PRINCIPLES OF ENSURING THE SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS IN THE CONTEXT OF CYBER THREATS

Lucian SCÎRTOCEA,
Ph.D. Candidate, National Defense University "Carol I", Bucharest, Romania.
E-mail: lucian.scirtocea@yahoo.com

Abstract*: Considering the NATO and EU membership and in the context of new cyber threats, ensuring the security of information and communication systems has become a priority for both public institutions, private companies and the Romanian Army. In this article the aim is to present the main functions and principles of ensuring the security of information and communication systems in the context of the evolution of the IT @ C field.*

Keywords*: information security; cyber threats; computer and communication systems; cyber attacks; security of information and communication systems.*

Introduction

Cyber threats represent a new generation of security challenges, aimed at the defense capacity of states, as well as the personal security of citizens.

Information security threats are a problem for many individuals and also for corporations.

The Internet is the main source of IT security risks. Cyber attacks organizations have an increasing frequency: malicious websites, phishing or spam emails or unsecured cloud computing services can be sources of viral and malware infections, which can lead to the deletion or theft of key data and , by default, to financial losses.

In recent years, the complexity of cyber attacks has increased rapidly, in a single attack being incorporated both elements of social engineering and malicious software.

The sources of cyber threats are diverse: hackers, frustrated people, criminal organizations, extremist political groups, fanatical religious movements, hostile intelligence services, terrorist groups.

Cyber attack is the act of exploiting or attempting to exploit a vulnerability of a computer system without authorization.

Current cyber attacks are able to bypass conventional security mechanisms, by using techniques aimed at identifying and exploiting existing vulnerabilities, obtaining an access point in computer and communication systems, downloading computer viruses without users detecting abnormal behavior.

1. The main types of cyber security threats

Cyber threats are becoming an increasingly present impediment in our lives. Moreover, some experts are already talking about a "cyber war", the most eloquent the example being the United States, which is already dealing with the conflict cybernetic as a terrorist type (ENISA, 2012, 2).

The cyber threats in the online environment are constantly growing. Cyberspace it will always be animated by the continuous race between the attackers and those affected by them attacks.

The following are the *main cyber threats to the security of information and communications systems*.

Drive-by exploits can automatically exploit vulnerabilities in software installed on a PC without interacting with the right user. When a user visits a site that contains drive-by exploits (ENISA, 2012, 2), vulnerabilities can be exploited in browser, its plugins or the operating system to install malware on your PC without the user's knowledge.

There is also the possibility that the attackers will design a special site (fake website or even phishing) to infect those who access it. Thus, to determine users accustomed to visiting it, they resort to a strategy based on spam emails (sending of unsolicited messages by the recipient) containing links to such illegal sites.

Malware is malicious software such as spyware, ransomware, viruses and worms (The University of North Dakota, n.d.). Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software.

Code injection: This type of threat includes well-known attack techniques against applications web, such as SQL Injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc. Attackers who generate such an attack try to extract data, steal credentials, take control of the targeted web server or promote malicious activities through through the exploitation of web application vulnerabilities. In recent years, the most common vector of attack against web applications is SQL Injection (ENISA, 2012,14-15). Moreover, such attacks are popular among groups hacktivist.

Denial of Service. A *Denial of Service attack* is an attempt to affect the availability of some computer or electronic communications systems/services (Orion Cassetto, 2019). The target system is attacked by the transmission of a very large number of illegitimate requests, which consume resources its hardware or software, making it unavailable to legitimate users.

Social engineering attacks act by misleading users into disclosing confidential information. Social engineering attacks include: Phishing attacks, Spear Phishing attacks as well as homograph attacks. Phishing is a form of online scam that involves the use of scams techniques for manipulating the identity of some people/organizations to obtain some material advantages or confidential information **(**William Goddard, 2021). Spear phishing attacks are a specific form of phishing in which attackers target privileged users within certain organizations. Homographic attack: represents the way in which the aggressor creates a fake website, with a web address very similar to a legitimate website and with the same look. Users are not aware that they are not on a real site buying non-existent goods and services by entering confidential data specific to the cards used.

Ransomware. A type of threat that takes the form of fake software used by cybercriminals to lure users to their malicious purposes (Linda Rosencrance, n.d.). The victim's computer is locked, typically by encryption, which keeps the victim from using the device or data that's stored on it. To regain access to the device or data, the victim has to pay the hacker a fee. This type of threat is spread by various methods such as social techniques engineering, trojans, exploitation of vulnerabilities (especially java).

Spam. Unsolicited electronic messages, most often commercial in nature, that do advertising for products and services, being used by the e-marketing industry and by to site owners with indecent content (ENISA, 2013, 26). Usually spam messages are sent by computers infected with Trojans, which do part of a botnet (a network of compromised computers used to send spam, or attacks on websites without the knowledge of computer owners respectively). Spam messages, although not a malicious program in themselves, can include attachments containing such programs, and send users to dangerous websites.

Sources of cyber threats. Common sources of cyber threats include: *state-sponsored—cyberattacks by countries, terrorists, industrial spies, organized crime groups-criminal groups, hackers, malicious insider* and *cyber espionage.*

2. Functions of securing information and communications systems

In order to reduce the threats, vulnerabilities and risks to which information and communication systems are subjected, the security of these systems requires the fulfillment of certain functions, namely:

Ensuring confidentiality, as a specific function, involves protecting a channel for transmitting information flow and information against unauthorized access and disclosure.

Confidentiality ensures the access of users only to the information specified in the security certificate. Authorized and official access to information for the institution's staff is materialized in a security certificate and in the "need to know" according to the duties of the position in the organizational chart.

Through privacy services, data and information from computer and communications networks will not be accessed and will only be available to authorized users, even if this data is stored on servers or workstations, respectively in transit through the network.

The second function, *ensuring integrity*, involves keeping information unaltered in the face of threats of any kind, as an action of human, technical or natural factors.

Integrity is ensured through the use of specific security mechanisms and products such as encryption, digital signatures and mechanisms for detecting unauthorized access.

In communications networks, integrity is approached in a specific form, called authenticity, which ensures that the data source is verified, the workstation and the user are determined, and that the time at which the operation was performed is integrated.

Integrity is ensured by:

- prevention of actions to modify data or programs by unauthorized users;
- preventing the operation of unauthorized or incorrect modifications, made by authorized operators;
- maintaining data and programs unaltered.

Ensuring availability is the function of ensuring access to and use of information and services only by authorized personnel.

Lack of availability may result in refusal of service or loss of data processing capacity, as a result of natural disasters (earthquakes, floods, etc.), accidents (fires or floods caused) or destructive human actions.

Four types of measures are important to *ensure availability*: *physical, technical, administrative and personal*.

Physical measures include access control, fire and humidity detection and warning systems, data restoration facilities outside the data processing premises.

Technical measures include fault tolerance mechanisms, access control applications to prevent disruption of services by unauthorized persons.

Administrative measures are in addition to issues related to access control policies and operating procedures, emergency response plans, user training.

Proper training of operators, programmers and security personnel is a special measure, with a focus on avoiding various availability disruptions.

As a distinct function, ***non-repudiation*** involves the removal of any uncertainty about the source or destination of a transmission, by using a reliable record that can be independently verified to establish the origin/destination of the information.

Without being a specific function, ***the audit*** represents the creation and protection of some necessary evidence in the process of investigating some facts generating security events.

The tests can be concretized in activity logs that record a series of data such as: usernames, time moments and associated actions.

Very important in ensuring the functioning of information and communication systems, ***restoration*** is the function by which information and systems can be restored if their availability has been affected.

Restoration is perhaps the most important function if one or more functions have not been performed successfully.

The functions of ensuring the security of information and communication systems become critical when we approach the fields of national security, as failure to fulfill any of them leads to compromise of information and failure to perform missions, resulting in loss of life, property damage and rescheduling or performing additional missions.

3. Principles of ensuring the security of information and communication systems

Understanding and assuming the general p*rinciples of ensuring the security of information and communication systems* will help security officials in the process of implementing security measures, to allocate the necessary resources to these specific activities, to understand the role of analysis and the tools it offers.

The first principle of ensuring security is that *there is no absolute security*. Understanding this principle will help staff with responsibilities in the field of information and communication systems security to decide what information is considered vital for different organizations as well as how to allocate the necessary funds for the implementation of security measures.

The second principle refers to ensuring the security of information and communication systems *must be carried out in depth, layered,* as a strategy to ensure information security.

Ensuring layered security is known as securing information in deep electronic format. This way of ensuring security provides us with the three elements necessary to protect information infrastructures, namely: prevention, detection and response. This in-depth security strategy provides us with answers to how to design these three elements so that if one element is weakened or outdated the other two elements can be further strengthened.

The third principle of ensuring the security of information and communication systems refers *to the fact that in the moments when they are left unattended, the staff tends to take the most uninspired decisions regarding the security of information in electronic format.*

Another principle, the fourth, refers to the fact that ensuring the security of information and communication systems depends on *two major components, namely those on the operation of information systems according to the established parameters and on ensuring the functions and requirements to be implemented and tested on these computer systems*. Functionality describes what a computer system needs to do. Assurance of functions and requirements describes how the system should be implemented and tested.

The fifth principle refers to *risk analysis.* This principle is very important to understand and analyze the value of information conveyed in information and communication systems in order to be able to design an appropriate security system following the analysis of existing threats to the information system and the amount of resources needed to do so.

The sixth principle refers to the fact that the *oversupply of measures to ensure the security of information and communication systems or the increase in the complexity of measures designed at the level of IT infrastructure*s without taking into account the value of the information we want to protect can be an enemy of security. rather, they can be a security vulnerability.

The seventh principle maintains that the *lack of decision-making, uncertainty and doubts of those responsible for ensuring security* are not the preconditions for a good way of carrying out specific activities.

The eighth principle refers to t*he way in which personnel, processes and technologies are designed and implemented to ensure the security of information and communication systems.* These measures are carried out in such a way that certain activities are carried out in compliance with the rule of the two. In order to avoid the occurrence of certain errors of judgment, activities are implemented so that certain activities are supervised by staff with responsibilities in the field of security assurance.

The last principle refers to the way in which *discussing vulnerabilities in ensuring the security of information and communication systems is a beneficial thing for ensuring security.* Hiding certain security vulnerabilities is not a solution.

In conclusion, understanding and implementing these principles listed above will help staff with responsibilities in ensuring the security of information and communication systems on how to manage information infrastructures in terms of security. How to allocate, distribute and plan the resources needed to ensure the security of information and communication systems is in fact the great challenge that security staff face.

4. The main preventive measures and technical solutions against cyber threats and attacks

In order to *prevent increasingly advanced security threats*, it is important that cybersecurity is addressed in a stratified manner. The main steps to ensure the security of information and communication systems are:

- risk assessment;
- social mentions Monitoring;
- reducing vulnerabilities.

The main measures meant to prevent and treat the effects of *counter cyber threats* are the following:

- securing the IT system;
- creating security plans;
- disaster recovery plans;
- risk assessment;
- email security;
- implement authentication solutions;
- endpoint security;
- firewall and network protection;
- reducing IT security vulnerabilities;
- web content filtering;
- data protection.

For the prevention and successful management of these threats, any organization it should consider implementing and complying with security policies cybernetics comprising:

- installation of antivirus solutions;
- implementation of appropriate data back-up policies;
- constantly updating the applications and systems used for removal possible vulnerabilities;

- restricting access from the Internet to internal systems (restriction RDP access and implementation of two-step authentication, closing unused ports for exposed IT&C systems;
- changing passwords regularly and ensuring a level of complexity their high;
- establishing an awareness policy regarding activities subsumed to social engineering (phishing, spear phishing);
- segmentation of IT&C networks;
- establishing a cyber security incident response plan in view increasing the level of resilience of IT&C systems and networks within the organization;
- training and testing employees' reaction to cyber incidents.

We will introduce you below with some *Technical solutions*[1] (Google, Romanian intelligence service, Press releases, 2021) used to prevent *cyber attacks* on IT and communication infrastructures as follows:

- using an updated antivirus solution;
- update operating systems and all applications used;
- frequent change of passwords of all users, respecting the recommendations of complexity;
- periodic verification of all registered users, to identify new users, added illegally;
- backing up critical data on offline data carriers;
- keep encrypted data in the event that an decryption application may appear in the online environment.

Conclusions

Cybercriminals end up using more and more advanced methods for implement attack vectors that are undetectable and difficult to neutralize.

It is becoming increasingly clear that mobile technology is and will become more and more exploited by cybercriminals. Threats already known and run in the traditional IT space will also prevail on mobile terminals. Proliferation of devices mobile will lead to an increase in socially generated abuse mediate.

The criminal activity that takes place in the online environment is new to us at the moment perspectives: malware consumption, cyberhacking tools and services, the emergence of digital currency and anonymous payment services.

Organizations, public or private, that hold and manage personal data or who provide essential services to the population, will be the most targeted by the attackers cybernetics in search of financial gain.

In the future we will deal with the theft of credentials, including bank details, both of customers as well as employees, by sending phishing or spear emails phishing, or by compromising POS (point-of-sale).

Phishing/spear phishing will continue to be the preferred methods of distribution of malware, given the high success rate of this mechanism, generated in largely due to the non-application of security policies as well as the security culture, including cybernetics, insufficient users.

The field of ensuring information security in electronic format in the conditions of new cyber threats becomes a particularly important and complex activity to ensure the successful accomplishment of the missions entrusted and assumed by the Romanian Army, as a member of the NATO alliance.

[1] See: https://www.sri.ro/articole/atac-cibernetic-cu-aplicatia-ransomware-phobos

BIBLIOGRAPHY:

CASSETTO, Orion. June 25, 2019. "21 Top Cybersecurity Threats and How Threat Intelligence Can Help". URL: https://www.exabeam.com/information-security/cyber-security-threat

ENISA, 2012, Threat Landscape.

ENISA, 2013,Threat Landscape.

ENISA, 2021, Methodology for sectoral Cybersecurity Assessments.

GODDARD, William. May 18, 2021. "Top 25 Cyber Security Threats", URL: https://itchronicles.com/information-security/top-25-cyber-security-threats

Romanian Intelligence Service. 2021. Press releases, "Cyber attack with PHOBOS ransomware application". URL: https://www.sri.ro/articole/atac-cibernetic-cu-aplicatia-ransomware-phobos

ROSENCRANCE, Linda. n.d. "Top 10 types of information security threats for IT teams ", URL: https://searchsecurity.techtarget.com/feature/Top-10-types-of-information-security-threats-for-IT-teams

The University of North Dakota, n.d.. "7 Types of Cyber Security Threats". URL: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats